

CONSTRUCTION OF $B_h[g]$ SETS IN PRODUCT OF GROUPS

DIEGO RUIZ AND CARLOS TRUJILLO

DEPARTMENT OF MATHEMATICS

UNIVERSIDAD DEL CAUCA

POPAYÁN-COLOMBIA

df Ruiz@unicauca.edu.co, trujillo@unicauca.edu.co

ABSTRACT. A subset \mathcal{A} of an abelian group G is a $B_h[g]$ set on G if every element of G can be written at most g ways as sum of h elements in \mathcal{A} . In this work we present constructions of $B_h[g]$ sets on the abelian groups $(\mathbb{F}^h, +)$, $(\mathbb{Z}^d, +)$, and $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$, for $d \geq 2$, $h \geq 2$, and $g \geq 1$, with \mathbb{F} any field.

Keywords and phrases. Sidon sets, $B_h[g]$ sets.

2000 Mathematics Subject Classification. 11B50, 11B75.

1. INTRODUCTION

Let g and h be positive integers with $h \geq 2$, and let G be an abelian additive group denoted by $(G, +)$. If $\mathcal{A} = \{a_1, \dots, a_k\} \subseteq G$, we say \mathcal{A} is a $B_h[g]$ on G , and it is denoted by $B_h[g]/G$, if every element of G can be written at most g ways as sum of h elements in \mathcal{A} , that is, if given $x \in G$, the amount of solutions of the equation $x = a_1 + \cdots + a_h$ is at most g up to rearrangement of summands, where $a_1, \dots, a_h \in \mathcal{A}$. If $g = 1$, \mathcal{A} is called a B_h set, and when $g = 1$ and $h = 2$ it is called a Sidon set.

Let $F_h(G, g)$ denote the largest cardinality of a $B_h[g]$ on G , i.e.,

$$F_h(G, g) := \max\{|\mathcal{A}| : \mathcal{A} \in B_h[g]/G\},$$

where $|\mathcal{X}|$ denotes the cardinality of a finite set \mathcal{X} . If $g = 1$ we write $F_h(G)$ instead of $F_h(G, 1)$. Furthermore, if G can be written as the direct product of $d \geq 2$ abelian groups and \mathcal{A} is a $B_h[g]$ set on G , sometimes we say that \mathcal{A} is a d -dimensional $B_h[g]$ set on G . Let $N \in \mathbb{N}$ and define $[0, N - 1] := \{0, 1, \dots, N - 1\}$. If $G = (\mathbb{Z}^d, +)$ we define

$$F_h^d(N, g) := \max\{|\mathcal{A}| : \mathcal{A} \subseteq [0, N - 1]^d, \mathcal{A} \in B_h[g]\},$$

where \mathbb{Z}^d denotes the set of all d -tuples of integers numbers, and $[0, N - 1]^d$ denotes the cartesian product of $[0, N - 1]$ with itself d times.

The main problem in the study of $B_h[g]$ sets consists of establishing the largest cardinality of a $B_h[g]$ set on a finite group G . Using constructions we can find lower bounds for

$F_h(G, g)$, while with counting and combinatorial techniques we can state upper bounds. In this work we focus in constructions from which we obtain some known lower bounds for $F_h(G, g)$ on particular groups G , while other works as [1], [2], [3], are focused in state upper bounds.

Different works have introduced constructions of $B_h[g]$ sets for particular values of h , and g . On $(\mathbb{Z}, +)$, the most obvious construction of Sidon sets is given by Mian–Chowla using the greedy algorithm [4]. This result is generalized for any $h \geq 2$ and any $g \geq 1$ in [5].

Other constructions of B_h sets are due to Rusza, Bose, Singer, and Erdős & Turán. Rusza constructs a Sidon set on the group $(\mathbb{Z}/(p^2 - p), +)$ for p prime. Bose's construction initially consider $h = 2$ but is generalized to any $h \geq 2$ on the group $(\mathbb{Z}_{q^{h-1}}, +)$, where q is a prime power. Similarly to Bose, Singer constructs a B_h set with $q + 1$ elements on $(\mathbb{Z}_{(q^{h+1}-1)/(q-1)}, +)$. Actually this construction can be established using a B_{h+1} set obtained from Bose's construction [6]. Finally, Erdős & Turán construct Sidon sets on $(\mathbb{Z}, +)$ based on quadratic residues modulo a fixed prime p . For details of these constructions see [5].

In dimension $d = 2$ some constructions are due to Welch, Lempel, Golomb [7], Trujillo [8], and C. Gómez & Trujillo [6]. Welch constructs Sidon sets with $p - 1$ elements on the groups $(\mathbb{Z}_{p-1} \times \mathbb{Z}_p, +)$, $(\mathbb{Z}_p \times \mathbb{Z}_{p-1}, +)$, which is generalized in [9] to the groups $(\mathbb{Z}_{q-1} \times \mathbb{F}_q, +)$ and $(\mathbb{F}_q \times \mathbb{Z}_{q-1}, +)$, respectively, being \mathbb{F}_q the finite field with q elements. Golomb's construction gives Sidon sets with $q - 2$ elements on the group $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$, while Lempel's construction is a particular case of Golomb. In [8] Trujillo presents an algorithm that allows us to obtain Sidon sets on $(\mathbb{Z} \times \mathbb{Z}, +)$ from a given Sidon set on $(\mathbb{Z}, +)$. Finally, C. Gómez & Trujillo construct B_h sets on $(\mathbb{Z}_p \times \mathbb{Z}_{p^{h-1}-1}, +)$.

In higher dimensions, Cilleruelo presents how to map Sidon sets in \mathbb{N} to Sidon sets in \mathbb{N}^d for $d \geq 2$, and furthermore he obtains a relation between the functions $F_h(N^d)$ and $F_h^d(N)$ [2].

The main object of this work is to present constructions of d -dimensional $B_h[g]$ sets for $d \geq 2$ on special abelian groups. First construction uses the elementary symmetric polynomials and the Newton's identities to generalize one construction done initially for $d = 2$ (original construction can be found in [10]). In the second construction we generalize Trujillo's algorithm given in [8] to any dimension d and all $h \geq 2, g \geq 1$, obtaining lower bounds for $F_h^d(N, g)$ from a known lower bounds for $F_h(N^d, g)$. Finally, using homomorphism between abelian groups, we construct d -dimensional $B_h[g']$ sets from d -dimensional $B_h[g]$ sets, with g a divisor of g' .

The remainder of this work is organized as follows: Section 2 describes a construction of B_h sets on $(\mathbb{F}^h, +)$, where \mathbb{F} is any field and \mathbb{F}^h denotes the set of all h -tuples of elements of \mathbb{F} . Section 3 presents a construction of $B_h[g]$ sets on $(\mathbb{Z}^d, +)$, and in Section 4 we construct $B_h[g]$ sets on $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$ and show a generalization of Golomb Costas array construction. Finally, Section 4 describes the concluding remarks of this work.

2. CONSTRUCTION OF B_h SETS ON $(\mathbb{F}^h, +)$

Let p be a prime number. It is easy to prove that $\mathcal{A} := \{(x, x^2) : x \in \mathbb{Z}_p\}$ is a B_2 set on $(\mathbb{Z}_p \times \mathbb{Z}_p, +)$ [10]. In this section we generalize this construction for any dimension $d > 2$ and any number of summands $h > 2$. First we introduce the following notations and definitions.

Let n be a positive integer. The elementary symmetric polynomials in the n variables x_1, \dots, x_n , written by $\sigma_k(x_1, \dots, x_n)$ for $k = 1, \dots, n$, is defined as

$$\sigma_k(x_1, \dots, x_n) := \sum_{1 \leq j_1 < \cdots < j_k \leq n} x_{j_1} \cdots x_{j_k}.$$

If $k = 0$ we consider $\sigma_0(x_1, \dots, x_n) = 1$. For instance, if $n = 3$

$$\begin{aligned} \sigma_0(x_1, x_2, x_3) &= 1, \\ \sigma_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3, \\ \sigma_2(x_1, x_2, x_3) &= x_1x_2 + x_1x_3 + x_2x_3, \\ \sigma_3(x_1, x_2, x_3) &= x_1x_2x_3. \end{aligned}$$

Note that the elementary symmetric polynomials appear in the expansion of a linear factorization of a monic polynomial as follows

$$\prod_{j=1}^n (\lambda - x_j) = \sum_{k=0}^n (-1)^k \sigma_k(x_1, \dots, x_n) \lambda^{n-k}.$$

Now, if $p_k(x_1, \dots, x_n) = x_1^k + \cdots + x_n^k$, the Newton's identities are given by

$$(1) \quad k\sigma_k(x_1, \dots, x_n) = \sum_{i=1}^k (-1)^{i-1} \sigma_{k-i}(x_1, \dots, x_n) p_i(x_1, \dots, x_n),$$

for each $1 \leq k \leq n$ and for an arbitrary number n of variables. With notations and definitions above we can state the following theorem.

Theorem 1. *Let \mathbb{F} be a field with characteristic zero or $p > h$. The set*

$$\mathcal{A} := \{(x, x^2, \dots, x^h) : x \in \mathbb{F}\},$$

is a B_h set on $(\mathbb{F}^h, +)$.

Proof. Let $s \in \mathbb{F}^h$. Suppose there exist two different representations of s as sum of h elements of \mathcal{A} as follows

$$s = (a_1, \dots, a_1^h) + \dots + (a_h, \dots, a_h^h) = (b_1, \dots, b_1^h) + \dots + (b_h, \dots, b_h^h),$$

where $a_i, b_i \in \mathbb{F}$ for $i = 1, \dots, h$. Note that for all $k = 1, \dots, h$, $\sum_{i=1}^h a_i^k = \sum_{i=1}^h b_i^k$. Because $p_k(a_1, \dots, a_h) = \sum_{i=1}^h a_i^k$ and $p_k(b_1, \dots, b_h) = \sum_{i=1}^h b_i^k$, from (1) recursively we have $\sigma_i(a_1, \dots, a_h) = \sigma_i(b_1, \dots, b_h)$, for all $i = 1, \dots, h$, i.e.,

$$\begin{aligned} a_1 + \dots + a_h &= b_1 + \dots + b_h, \\ a_1 a_2 + \dots + a_{h-1} a_h &= b_1 b_2 + \dots + b_{h-1} b_h, \\ &\dots \\ a_1 \dots a_h &= b_1 \dots b_h, \end{aligned}$$

implying that the elements of the sets $\{a_1, \dots, a_h\}$ and $\{b_1, \dots, b_h\}$ are roots of the same polynomial $q(x)$ on $\mathbb{F}[x]$, i.e.,

$$q(x) = (x - a_1) \dots (x - a_h) = (x - b_1) \dots (x - b_h).$$

Because $\mathbb{F}[x]$ is a unique factorization domain we have $\{a_1, \dots, a_h\} = \{b_1, \dots, b_h\}$, what implies that cannot be possible to have two different representations of $s \in \mathbb{F}$ as sum of h elements of \mathbb{F}^h . That is, \mathcal{A} is a B_h set on $(\mathbb{F}^h, +)$. \square

Now we consider the case when \mathbb{F} is the finite field \mathbb{F}_q , with $q = p^n$ for some $n \in \mathbb{N}$ and p prime. Note that the groups $(\mathbb{F}_{p^n}, +)$ and $(\mathbb{F}_p^n, +)$ are isomorphic, because if θ is a root of an irreducible polynomial on \mathbb{F}_{p^n} in an extension field, the function

$$(2) \quad \begin{array}{ccc} \phi : & \mathbb{F}_{p^n} & \rightarrow \mathbb{F}_p^n \\ & a_0 + \dots + a_{n-1} \theta^{n-1} & \mapsto (a_0, \dots, a_{n-1}) \end{array}$$

defines an isomorphism between them. Using this function we can state the following result.

Corollary 1. *For all $p > h$ prime and for all $n \in \mathbb{N}$ there exists a B_h set with p^n elements on $(\mathbb{Z}_p^{hn}, +)$.*

Proof. It follows immediately from the isomorphism ϕ between $(\mathbb{F}_{p^n}, +)$ and $(\mathbb{F}_p^n, +)$ given in (2) and from Theorem 1. \square

To illustrate these results consider the following example.

Example 1. Consider $h = n = 2$ and $p = 3$. Let $p(x) = x^2 + 1$ be an irreducible polynomial on \mathbb{Z}_3 . Suppose that θ is a root of $p(x)$ in an extension field of \mathbb{Z}_3 . The field with 9 elements is given by

$$\begin{aligned}\mathbb{F}_9 &= \{a + b\theta : a, b \in \mathbb{Z}_3\} \\ &= \{0, 1, 2, \theta, \theta + 1, \theta + 2, 2\theta, 2\theta + 1, 2\theta + 2\}.\end{aligned}$$

From Theorem 1 we have that

$$\mathcal{A} = \left\{ \begin{array}{l} (0, 0), (1, 1), (2, 1), (\theta, 2\theta + 1), (\theta + 1, \theta + 2), \\ (\theta + 2, 2), (2\theta, 2\theta + 1), (2\theta + 1, 2), (2\theta + 2, \theta + 2) \end{array} \right\}$$

is a Sidon set on $(\mathbb{F}_3 \times \mathbb{F}_3, +) = (\mathbb{F}_3^2, +)$. Furthermore, by Corollary 1,

$$\mathcal{B} = \left\{ \begin{array}{l} (0, 0, 0, 0), (0, 1, 0, 1), (0, 2, 0, 1), (1, 0, 2, 1), (1, 1, 1, 2), \\ (1, 2, 0, 2), (2, 0, 2, 1), (2, 1, 0, 2), (2, 2, 1, 2) \end{array} \right\}$$

is a Sidon set on $(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, +) = (\mathbb{Z}_3^4, +)$.

3. CONSTRUCTION OF $B_h[g]$ SETS ON $(\mathbb{Z}^d, +)$

In this section we construct $B_h[g]$ sets for all $h, g \geq 2$ on $(\mathbb{Z}^d, +)$. This construction generalizes an algorithm introduced by Trujillo in [8] which allowed us to construct Sidon sets on $(\mathbb{Z} \times \mathbb{Z}, +)$ from a Sidon set on $(\mathbb{Z}, +)$. Our generalization allow us to construct d -dimensional $B_h[g]$ sets for all $h, g \geq 2$ and any dimension d , and show us a way to map $B_h[g]$ sets on $(\mathbb{Z}, +)$ into $B_h[g]$ sets on $(\mathbb{Z}^d, +)$.

Let d, N be positive integers greater than 1, and \mathcal{A} a subset of \mathbb{Z}^+ . If $a \in \mathcal{A}$ we write

$$[a]_N = (n_k, \dots, n_1, n_0)_N$$

to represent the number $a = n_k N^k + \dots + n_1 N + n_0$ in base N notation, where k is a nonnegative integer and $0 \leq n_j \leq N - 1$, for $j = 0, 1, \dots, k$. We denote the set obtained from the representation of each element of \mathcal{A} in base N as $[\mathcal{A}]_N$. Because every positive integer can be written uniquely in base N , then

$$(3) \quad |\mathcal{A}| = |[\mathcal{A}]_N|.$$

Note that if $\mathcal{A} \subseteq [0, N^d - 1]$, then $[\mathcal{A}]_N \subseteq [0, N - 1]^d$.

With these notations we can state the following result.

Theorem 2. *If \mathcal{A} is a $B_h[g]$ set contained in $[0, N^d - 1]$, then $[\mathcal{A}]_N$ is a $B_h[g]$ set contained in $[0, N - 1]^d$. Furthermore, $|[\mathcal{A}]_N| = |\mathcal{A}|$.*

Proof. In (3) we established that $|\mathcal{A}_N| = |\mathcal{A}|$. Now we prove that \mathcal{A}_N is a $B_h[g]$ set on $[0, N-1]^d$.

Let s be a d -tuple in \mathbb{Z}^d obtained as sum of h elements in \mathcal{A}_N . Furthermore, suppose there exist $g+1$ representations of s as follows

$$(4) \quad s = [a_{1,1}]_N + \cdots + [a_{1,h}]_N = \cdots = [a_{g+1,1}]_N + \cdots + [a_{g+1,h}]_N,$$

where $a_{i,j} \in \mathcal{A}$ for all $1 \leq i \leq g+1$, $1 \leq j \leq h$. Consider the representation of each $a_{i,j} \in \mathcal{A}$ in base N notation as $[a_{i,j}]_N = (n_{(d-1,i,j)}, \dots, n_{(0,i,j)})$. Note that for any $1 \leq i \leq g+1$

$$\begin{aligned} [a_{i,1}]_N + \cdots + [a_{i,h}]_N &= (n_{(d-1,i,1)}, \dots, n_{(0,i,1)}) + \cdots + (n_{(d-1,i,h)}, \dots, n_{(0,i,h)}) \\ &= (n_{(d-1,i,1)} + \cdots + n_{(d-1,i,h)}, \dots, n_{(0,i,1)} + \cdots + n_{(0,i,h)}) . \end{aligned}$$

Furthermore

$$(n_{(d-1,i,1)} + \cdots + n_{(d-1,i,h)}) N^{d-1} + \cdots + (n_{(0,i,1)} + \cdots + n_{(0,i,h)}) = a_{i,1} + \cdots + a_{i,h}$$

what implies from (4) that

$$(5) \quad a_{1,1} + \cdots + a_{1,h} = \cdots = a_{g+1,1} + \cdots + a_{g+1,h}.$$

Because \mathcal{A} is a $B_h[g]$ set, from (5) there exist ℓ, m with $\ell \neq m$ and $1 \leq \ell, m \leq g+1$, such that

$$\{a_{\ell,1}, \dots, a_{\ell,h}\} = \{a_{m,1}, \dots, a_{m,h}\}.$$

Since representation in base N notation is unique, then

$$\{[a_{\ell,1}]_N, \dots, [a_{\ell,h}]_N\} = \{[a_{m,1}]_N, \dots, [a_{m,h}]_N\},$$

which implies that cannot be possible to have $g+1$ representations of s as sum of h elements of \mathcal{A} . Therefore \mathcal{A}_N is a $B_h[g]$ set contained in $[0, N-1]^d \subset (\mathbb{Z}^d, +)$. \square

As an illustration of Theorem 2 consider the following example.

Example 2. Note that $\mathcal{A} = \{1, 2, 7\}$ is a Sidon set on $(\mathbb{Z}_8, +)$. In [8] Trujillo constructs a $B_2[2]$ set on $(\mathbb{Z}, +)$ as follows

$$\mathcal{B} := \mathcal{A} \cup (\mathcal{A} + m) \cup (\mathcal{A} + 3m) = \{1, 2, 7, 9, 10, 15, 25, 26, 31\},$$

where $m = 8$. Because $\mathcal{B} \subseteq [0, 2^5 - 1]$,

from Theorem 2 we have that

$$[\mathcal{B}]_2 = \left\{ \begin{array}{l} (0, 0, 0, 0, 1), (0, 0, 0, 1, 0), (0, 0, 1, 1, 1), (0, 1, 0, 0, 1), (0, 1, 0, 1, 0), \\ (0, 1, 1, 1, 1), (1, 1, 0, 0, 1), (1, 1, 0, 1, 0), (1, 1, 1, 1, 1) \end{array} \right\}$$

is a $B_2[2]$ set contained in $[0, 1]^5$.

Note also that $\mathcal{B} \subseteq [0, 6^2 - 1]$, so the set

$$[\mathcal{B}]_6 = \{(0, 1), (0, 2), (1, 1), (1, 3), (1, 4), (2, 3), (4, 1), (4, 2), (5, 1)\}$$

is a $B_2[2]$ set contained in $[0, 5]^2$.

4. CONSTRUCTION OF $B_h[g]$ SETS ON $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$

In this section we present a generalization of construction performed by Trujillo et. al. in [11], where the authors construct in dimension $d = 1$, $B_2[g]$ sets from special Sidon sets. We extend such construction for all $d > 1$, and all $h \geq 2$. In order to introduce last construction we need the following auxiliary lemma.

Lemma 1. *Let $\phi : G \rightarrow G'$ be a homomorphism between abelian groups G and G' . If $|Ker(\phi)| = g'$ and \mathcal{A} is a $B_h[g]$ set on G , then $\phi(\mathcal{A})$ is a $B_h[gg']$ set on $\phi(G)$, where gg' denotes the product between g and g' .*

The proof of this result can be found in detail in [12]. Now, let m_1, \dots, m_d and g_1, \dots, g_d be positive integers. With Lemma 1 we can prove the following theorem.

Theorem 3. *Let \mathcal{B} a $B_h[g]$ set on $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$. If g_1, \dots, g_d are divisors of m_1, \dots, m_d , respectively, then*

$$\mathcal{A} := \left\{ \left(b_1 \bmod \frac{m_1}{g_1}, \dots, b_d \bmod \frac{m_d}{g_d} \right) : (b_1, \dots, b_d) \in \mathcal{B} \right\}$$

is a $B_h[gg_1 \cdots g_d]$ set on $\left(\mathbb{Z}_{\frac{m_1}{g_1}} \times \cdots \times \mathbb{Z}_{\frac{m_d}{g_d}}, + \right)$.

Proof. In Lemma 1, let $G = (\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$ and $G' = \left(\mathbb{Z}_{\frac{m_1}{g_1}} \times \cdots \times \mathbb{Z}_{\frac{m_d}{g_d}}, + \right)$ be two abelian groups and define $\phi : \mathcal{B} \subseteq G \rightarrow G'$ as $\phi(b_1, \dots, b_d) = \left(b_1 \bmod \frac{m_1}{g_1}, \dots, b_d \bmod \frac{m_d}{g_d} \right)$, with $(b_1, \dots, b_d) \in \mathcal{B}$. Note that ϕ is a homomorphism between G and G' . Furthermore, $(b_1, \dots, b_n) \in Ker(\phi)$ if and only if $\phi(b_1, \dots, b_n) = (0, \dots, 0)$, that is, if

$$\left(b_1 \bmod \frac{m_1}{g_1}, \dots, b_d \bmod \frac{m_d}{g_d} \right) = (0, \dots, 0).$$

Note that $b_i \bmod \frac{m_i}{g_i} = 0$ if and only if $b_i = k_i \frac{m_i}{g_i}$, for $k_i \in [1, g_i]$ and for all $i = 1, \dots, d$. It implies that $b_i \bmod \frac{m_i}{g_i} = 0$ in exactly g_i values. Thus, $|Ker(\phi)| = \prod_{i=1}^d g_i$, and as a result from Lemma 1 we have that \mathcal{A} is a $B_h[gg_1 \cdots g_d]$ set on $\left(\mathbb{Z}_{\frac{m_1}{g_1}} \times \cdots \times \mathbb{Z}_{\frac{m_d}{g_d}}, + \right)$. \square

To illustrate this result, for q prime power, in the following proposition we construct Sidon sets on $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$.

Proposition 1. *Let p be a prime and let n be a positive integer. If $q = p^n$; α, β are primitive elements of \mathbb{F}_q^* , and $a \in \mathbb{F}_q^*$, then*

$$\mathcal{G}(\alpha, \beta, a) := \{(i, \log_\beta(a - \alpha^i)) : i = 1, \dots, q-1, \alpha^i \neq a\}$$

is a Sidon set on $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$.

Proof. Let $a \in \mathbb{F}_q^*$. Suppose there exist $u, v, w, y \in \mathcal{G}(\alpha, \beta, a)$ such that $u + v = w + y$. By definition of $\mathcal{G}(\alpha, \beta, a)$, there exist $i, j, k, \ell \in [1, q-1]$ such that

$$(6) \quad (i, \log_\beta(a - \alpha^i)) + (j, \log_\beta(a - \alpha^j)) = (k, \log_\beta(a - \alpha^k)) + (\ell, \log_\beta(a - \alpha^\ell))$$

where $\alpha^i, \alpha^j, \alpha^k, \alpha^\ell$ are not equal to a . From (6) we have

$$(i + j) \equiv (k + \ell) \pmod{q-1},$$

$$\log_\beta(a - \alpha^i) + \log_\beta(a - \alpha^j) \equiv (\log_\beta(a - \alpha^k) + \log_\beta(a - \alpha^\ell)) \pmod{q-1},$$

what implies that $(a - \alpha^i)(a - \alpha^j) = (a - \alpha^k)(a - \alpha^\ell)$. So in \mathbb{F}_q^* we have

$$\begin{aligned} \alpha^i \alpha^j &= \alpha^k \alpha^\ell, \\ \alpha^i + \alpha^j &= \alpha^k + \alpha^\ell \end{aligned}$$

what means that α^i, α^j , and α^k, α^ℓ are roots of a polynomial $q(x) \in \mathbb{F}[x]$ of degree 2, i.e.,

$$q(x) = (x + \alpha^i)(x + \alpha^j) = (x + \alpha^k)(x + \alpha^\ell).$$

Therefore, $\{\alpha^i, \alpha^j\} = \{\alpha^k, \alpha^\ell\}$ and so $\{i, j\} = \{k, \ell\}$, implying that cannot be possible to have two representations of an element in $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ as sum of two elements of $\mathcal{G}(\alpha, \beta, a)$. That is, $\mathcal{G}(\alpha, \beta, a)$ is a Sidon set on $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$. \square

Example 3. *First we apply Proposition 1 to construct a Sidon set on $\langle \mathbb{Z}_{16} \times \mathbb{Z}_{16}, + \rangle$. Let $q = p = 17$, and let $\alpha = 3, \beta = 5$ be primitive elements of \mathbb{Z}_{17}^* . If $a = 1$, we have that*

$$\mathcal{G}(3, 5, 1) = \left\{ \begin{array}{l} (1, 14), (2, 10), (3, 2), (4, 1), (5, 4), (6, 13), (7, 15), (8, 6), \\ (9, 12), (10, 7), (11, 11), (12, 5), (13, 3), (14, 8), (15, 9) \end{array} \right\}$$

is a Sidon set on $(\mathbb{Z}_{16} \times \mathbb{Z}_{16}, +)$. Now, if $g_1 = g_2 = 2$, by Theorem 3,

$$\mathcal{A} = \left\{ \begin{array}{l} (1, 6), (2, 2), (3, 2), (4, 1), (5, 4), (6, 5), (7, 7), (0, 6), \\ (1, 4), (2, 7), (3, 3), (4, 5), (5, 3), (6, 0), (7, 1) \end{array} \right\}$$

is a $B_2[4]$ set on $(\mathbb{Z}_{16} \times \mathbb{Z}_{16}, +)$.

5. CONCLUDING REMARKS

As a result of constructions presented in this work we can obtain lower bounds and closed formulas for $F_h^d(G, g)$, for some abelian group G and some values of d, h and g .

Note from Theorem 1 and Corollary 1 that $F_2^h(\mathbb{F}_q^h) \geq q$ for q a prime power. Particularly if $h = 2$ and $q = p$ prime we have $F_2^2(\mathbb{Z}_p \times \mathbb{Z}_p) \geq p$, but it is easy to establish that $F_2^2(\mathbb{Z}_p \times \mathbb{Z}_p) = p$ [9]. A natural question to state is the follow: Can we obtain a similar result, as the last one, on the group $(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p, +)$? That is,

$$F_2^3(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \sim p^{3/2}?$$

Now, from Theorem 2 we can establish the following. Let d, g , and N be positive integers greater than or equal to 1 and be $h \geq 2$. Then

$$F_h(N^d, g) \leq F_h^d(N, g)$$

Particularly, if $d = 2$, $h = 2$, and $g = 1$ we have that $F_2^1(N^2) \leq F_2^2(N)$, what implies that good constructions of Sidon sets on \mathbb{Z} give us good lower bounds for Sidon sets on $\mathbb{Z} \times \mathbb{Z}$. Furthermore, an interesting work consists in to analyze the behavior of the difference $F_2^2(N) - F_2^1(N^2)$ when N grows. On the other hand, for $h = 2$, $g = 1$, and all $d \geq 1$ we get

$$\lim_{N \rightarrow \infty} \frac{F_2^d(N)}{N^{d/2}} = 1.$$

This result is obtained also in [2].

Finally, from Proposition 1 we can establish that $F_2^2(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) \geq q - 2$, what lead us to ask if is it possible to state that $F_2^2(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) = q - 1$?

Acknowledgment. The authors thank the Universidad del Cauca for the support under research project VRI 3744.

REFERENCES

- [1] J. Bravo, D. Ruiz, and C. Trujillo, "Cardinality of sets associated to B_3 and B_4 sets," *Revista colombiana de matemáticas*, vol. 46, no. 1, pp. 27–37, 2012.
- [2] J. Cilleruelo, "Sidon sets in \mathbb{N}^d ," *Journal of Combinatorial Theory Series A*, vol. 117, no. 7, pp. 857–871, 2010.
- [3] L. Rackham and P. Šarka, " B_h sequences in higher dimensions," *The Electronic Journal of Combinatorics*, vol. 17, no. 1, R35 (electronic), p. 15, 2010.
- [4] A. M. Mian and S. Chowla, "Solution of a problem of Erdős and Turán in additive-number theory," *Proc. Nat. Acad. Sci. India Series A*, vol. 14, pp. 3–4, 1944.
- [5] K. O'Bryant, "A complete annotated bibliography of work related to sidon sequences," *The electronic Journal of Combinatorics-Dynamic Surveys*, vol. 11, p. 39, 2004.

- [6] C. A. Gómez and C. Trujillo, “Una nueva construcción de conjuntos B_h modulares,” *Matemáticas: Enseñanza Universitaria*, vol. 19, no. 1, pp. 53–62, 2011.
- [7] S. Golomb and G. Gong, “The status of Costas arrays,” *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4260–4265, 2007.
- [8] C. Trujillo, *Sucesiones de Sidon*. PhD thesis, Universidad Politécnica de Madrid, España, 1998.
- [9] A. Gómez, D. Ruiz, and C. Trujillo, “Construcción de conjuntos de Sidon en dimensión dos,” in *XVIII Congreso Colombiano de Matemáticas*, Universidad Industrial de Santander (Colombia), Julio 2011.
- [10] J. Cilleruelo, “Conjuntos de enteros con todas las diferencias distintas,” *La Gaceta de la RSME*, vol. 11, no. 1, pp. 151–170, 2008.
- [11] C. Trujillo, G. Garcia, and J. Velasquez, “ $B_2^\pm[g]$ finite sets,” *Journal Of Algebra, Number Theory And Applications*, vol. 4, no. 3, pp. 593–604, 2004.
- [12] J. C. Gómez, “Construcción de conjuntos $B_h[g]$,” Master thesis, Universidad del Valle, Colombia, 2011.

DEPARTMENT OF MATHEMATICS—UNIVERSIDAD DEL CAUCA
CALLE 5 NO. 4–70 – POPAYÁN, COLOMBIA.
RESEARCH GROUP: ÁLGEBRA, TEORÍA DE NÚMEROS Y APLICACIONES, ERM – ALTENUA.